UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/091,735	06/24/1998	IAN DUNCAN BRAMHILL	36-1230	5276

7590 07/30/2003

NIXON & VANDERHYE
1100 NORTH GLEBE ROAD
8TH FLOOR
ARLINGTON, VA 222014714

EXAMINER
NGUYEN, CUONG H

ART UNIT	PAPER NUMBER
3625	

DATE MAILED: 07/30/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/091,735	Applicant(s) BRAMHILL ET AL.	
	Examiner CUONG H. NGUYEN	Art Unit 3625	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 May 2003*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8,12,14-18,21 and 28-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,12,14-18,21 and 28-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

1. This Office Action is the answer to a previous Appeal Brief, and the later filing amendment received on 5/02/2003; which papers have been placed of record.

2. Claims 1-30 are pending in this application; claims 9-11, 13, 19-20, 22-27 have been canceled; claims 34-38 have been added.

Response:

3. Applicants' arguments filed in the Appeal Brief received on 12/01/2003 with respect to claims 1-8, 12, 14-18, 21, 28-38 have been fully considered but are unpersuasive.

4. Spies et al. disclose about a difficulty in copying video data after data were distributed to a user (see Spies et al., 16:55-60).

5. On page 6, para.3 of the amendment received on 5/02/2003, the applicants argue that "Spies fails to disclose selectively controlling access to copy and save functions at the client in respect of data in its unprotected form" and "Spies fails to disclose restricting or preventing access to copy or save functions of data in its unprotected form". The examiner submits that although Spies may not expressly disclose these claimed language, Spies inherently includes this function (see Spies, 1:29-32). One with ordinary skill in the art would understand that this feature is clearly a capability of Spies et al.'s cryptographically protecting video content since "restricting or preventing access to copy or save functions of data in its unprotected form" is intend of use in cryptographically protecting data.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> ***(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.***

6. Re. to claims **30-38, 1-2, 5-8, 12, 14, 28:** They are rejected under 35 U.S.C. §103(a) as being unpatentable over **Spies** et al. (US Pat. 6,055,314),

Re. To claims **30-38**: **Spies** et al.'s patent is directed to a method/a server for protecting data (see Spies et al., 11:22-25) , comprising repetition steps/components of:

- a client requests specific data from a server, this is inherently done by "running a program portion at the client , the program portion generating and uploading to the server a request for access to data"; (see **Spies** et al., Fig.2)
- encrypting the data (see **Spies** et al., Fig. 3, ref. 66 wherein a video encryption device having said claimed capability);
- sending protected data to client (see **Spies** et al., claim 3 (i.e., 17:40-45)); and
- converting said protected data to unprotected forms, and preventing output data from being copied (this is analogous to a Spies' statement of "the

viewer is considered to have the ability to record and redistribute the video with little difficulty")(see **Spies** et al., Fig. 12, ref. 338, and 1:45-49)).

The examiner also submits that claim **32** is a "system" claim (a server) comprising:

- an input for receiving a request (see **Spies** et al. Fig.1, i.e., an I/O interface of computer system 44, 9:19-26);
- protecting means for cryptographically protecting the request data (see **Spies** et al., Fig. 3, ref. 66, 10:59-66, and 16:55-60).
- generating means for generating computer data/(note: "a program portion" is not distinguished from data/ instruction as in "system" claim 32); (see **Spies** et al., Fig. 9, ref. 206, and 8:31-33).

Spies et al. disclose about a difficulty in copying video data after data were distributed to a user (see Spies et al., 16:55-60).

Although Spies et al. do not expressly disclose claimed limitations, it would have been obvious to one of ordinary skill in the art at the time of invention to use sufficient ideas of **Spies** et al. 's invention to suggest above claimed steps because it would simply prevent any un-wanted change to original data; that serves a purpose for preventing original data.

A. Re. To claims **1, 28**: The examiner submits that they contain limitations as in rejected claims 31/32/34; therefore, similar rationales and reference set forth for 35 USC §103(a) rejections are applied.

B. As per claim **2**: The rationales & references for rejection of claim 1 are incorporated.

Spies et al. suggest a method that using encrypted data (see **Spies**, 16:55-64); the examiner submits that it is equivalent for "data protection" by encrypting.

C. Re. to claims **3-4:** The rationales & reference for rejection of claim 1 are incorporated.

Spies et al. also suggest a method that including a hashing algorithm for protecting data integrity (see **Spies et al.**, 7:31-35).

Because protecting crypto graphical data is also a form of protecting data (because both of them are merely data, and protecting crypto graphical data as claimed is analogous of protecting specific data); therefore, it is obvious for one with ordinary skill in the art to use Spies et al.'s teachings to perform a common step of protecting original data.

D. As per claim **5**: The rationales & reference for rejection of claim 1 are incorporated.

Spies et al. suggest a step of checking a destination/receiver/client before sending data (see **Spies**, claim 16).

E. As per claim **6**: The rationales & reference for rejection of claim 1 are incorporated.

Spies et al. suggest identifying a destination/ receiver/client to a server before sending data (see **Spies**, claim 16); the examiner submits that this has

been old, and well-known for artisan to identifying a receiver before sending anything to ensure a safety and correct transaction.

F. As per claim **12**: The rationales & reference for rejection of claim 1 are incorporated.

Spies et al. suggest that data are sent to a client through a network (see **Spies et al.**, Fig. 9, 11:22-25); the examiner submits that this has been old, and well-known for sending data via Internet.

G. As per claim **7**: The rationales & reference for rejection of claim 1 are incorporated.

The rationales & reference for rejection of claim 1 are incorporated.

Spies et al. obviously suggest:

- generating a program at a server (note: "a program" can be broadly interpreted as any general instruction/data);
- downloading said program to a client, and
- said client running said program to make a request.

These above limitations are obviously suggested in **Spies**, 16:19-40 & claim 11.

The examiner also submits that as a common practice, a server would distribute an available "template"/(program to request a particular software), then a user/client would enter a user/requester's name/address; name/ID of a specific software he needs and uploading those data to the server, those steps has been happening before this application's priority date.

H. As per claim **8**: The rationales & reference for rejection of claim 7 are incorporated.

Spies et al. also obviously suggest that a program/instruction is generated in response to a request for access to a specific data (see **Spies** et al., 16:20-39).

I. As per claim **14**: The rationales & reference for rejection of claim 7 are incorporated.

Spies et al. obviously suggest said program includes data concerning a cryptographic key, using said key to unprotect download data (see **Spies**, 16:19-54).

7. Claims **3-4**, **16** are rejected under 35 U.S.C. §103(a) as being unpatentable over **Spies** et al. (US Pat. 6,055,314), in view of **Rhoads** (US Pat. 5,841,978).

A. As per claim **3**: The rationales & reference for rejection of claim 1 are incorporated.

In addition to **Spies** et al.'s protecting any change to original data; **Rhoads** (US Pat. 5,841,978) also discloses a method that comprises protecting an integrity of data (e.g., see **Rhoads**, 57:5-35); please note that this analogous feature to claim 3 has been old, and well-known (e.g. data hashing technique, check-sum technique etc.).

Because protecting crypto graphical data is also a form of protecting data (because both of them are merely data, and protecting crypto graphical data as

claimed is analogous of protecting specific data); therefore, it is obvious for one with ordinary skill in the art to perform a common step of protecting original data.

B. As per claim **4**: The rationales & reference for rejection of claim 3 are incorporated.

Spies et al. also suggest a method that including a hashing algorithm for data integrity (see **Spies et al.**, 7:31-35); the examiner submits that this has been old, and well-known for hashing data.

It would have been obvious to one of ordinary skill in the art at the time of invention to combine ideas of **Rhoads** & **Spies** et al. to suggest above claimed steps because it would simply prevent any un-wanted change to original data; that serves a purpose for preventing original data.

C. As per claim **16**:

The rationales & reference for rejection of claim 1 are incorporated.

Spies et al. do not disclose about using stegano-graphical data.

However, to implement **Spies et al.**'s invention**, Rhoads**' patent gave ideas of utilizing stegano-graphical data (see **Rhoads**, claim 1).

It would have been obvious to one of ordinary skill in the art at the time of invention to have incorporated **Rhoads'** suggestion to **Spies** invention to suggest claimed step because it would use an available form of data such as stegano-graphic marked data for data protection purposes.

8. As per claim **15**: This claim is rejected under 35 U.S.C. §103(a) as being unpatentable over **Spies** et al. (US Pat. 6,055,314), in view of **Probst** (US Pat. 5,982,899).

The rationales & reference for rejection of claim 1 are incorporated.

Probst suggests what Spies 's missing in claim 15; he teaches a server and a client each hold data corresponding to a cryptographic key and a machine identifier for uniquely identifying a user/client, comprising:

- sending a challenge/query to a user/client (this feature is very well-known), such that it generates a signed response as a cryptographic function of the key and the machine identifier held therein (**Probst** suggests an analogous action for generating a combination feature of a key and a machine identifier, see **Probst**, the abstract),

- generating from the cryptographic key and machine identifier held associated with the server, a corresponding signed response as a cryptographic function of the key and the machine identifier (see **Probst**, the abstract, & 3:8-21 for suggesting a unique identifier by combining a key and a machine identifier);

- comparing the signed responses from the user/client and the server, performing the cryptographic protection of the data with the key (see **Probst**, 4:20-22, claims 5 and 15);

- converting/decrypting protected data into an unprotected form (see **Probst**, the abstract, claims 1, 15, and 3:8-21).

It would have been obvious to one of ordinary skill in the art at the time of invention to have incorporated **Probst's** suggestions to **Spies** invention to suggest above claimed steps because these are necessary and reasonable steps to verify a client by a server before deliver protected data.

9. As per claim **17**: This claim is rejected under 35 U.S.C. §103(a) as being unpatentable over **Spies** et al. (US Pat. 6,055,314), in view of the Official Notice. The rationales & references for rejection of claim 1 are incorporated.

Claim 17 contains a step of registering a client with a server.

The Official Notice is taken that in software renting business involving server/client (using Internet), a step of registering a client with a server has been old, & well-known for logging client identification as a record of each transaction.

10. As per claim **18**: This claim is rejected under 35 U.S.C. §103(a) as being unpatentable over **Spies** et al. (US Pat. 6,055,314), in view of **Crawford** (US Pat. 6,014,651).

The rationales & reference for rejection of claim 1 are incorporated.

Spies et al. suggest a method that:

- determining a user/client's machine identifier by hardware configuration, then transmitting said identifier to a server (see **Spies**, claim 15); the examiner submits that this step has been done prior to this pending invention.

In addition of **Spies et al.**'s patent, **Crawford's** patent also further gave an example for "combining an identifier with a content":

- combining an identifier with a key to form a unique identifier/determinator (see **Crawford**, claim15 wherein the act of combining is represented by a step of encrypting data with customer's identity, and providing said encrypted data);

- transmitting a (unique) identifier/determinator to the client for use (e.g., for identifying/transmitting data etc.)(note: transmitting a specific data to someone on Internet is old and well-known, and this step of transmitting data was done by both Spies et al. and Crawford).

It would have been obvious to one of ordinary skill in the art at the time of invention to have incorporated **Crawford's** suggestion to **Spies** et al. invention to suggest above claimed steps because using a unique identifier is convenient for data protection purposes.

11. As per claims **21, 28**: The examiner submits that they contain analogous limitations as claim 31; therefore, similar rationales and reference set forth for 35 USC 103(a) rejection of claim 31 are applied.

Conclusion

12. Claims 1-8, 12, 14-18, 21, 28-38 are unpatentable. Applicants' arguments (for old pending claims) are unpersuasive, and the Applicants' amendment (for newly added claims 34-38) necessitated new ground(s) of rejection presented in this Office Action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicants are reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Cuong H. Nguyen whose telephone number is 703-305-4553. The examiner can normally be reached on Mon.-Fri. from 7:15 AM to 3:15 PM (EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ms. Wynn Coggins, can be reached on (703)308-1344.

Any response to this action should be mailed to:

Amendments

Commissioner of Patents and Trademarks

Washington D.C. 20231

Cuonghnguyen
Primary Examiner